Bridging “Identity Islands” with Continuous, Contextual Identity Assurance

Kayvan Alikhani

RSA, Lead Strategist, Identity and Authentication

RSA

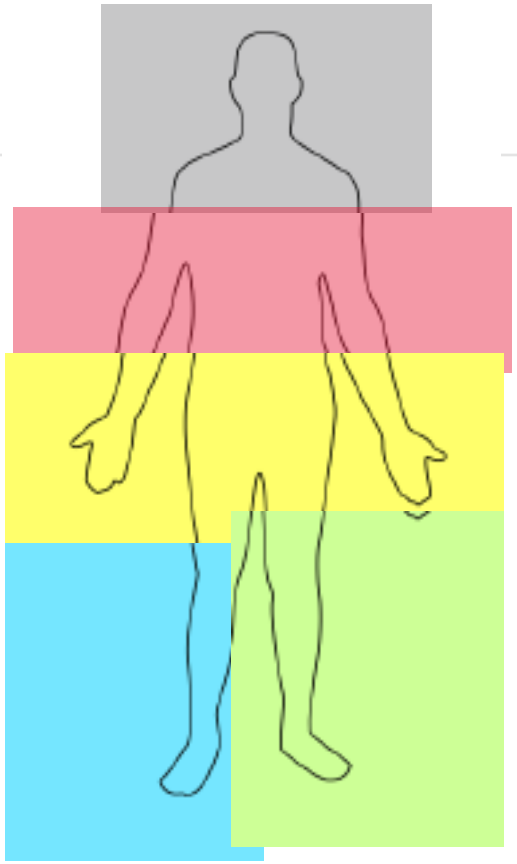
What we'll cover

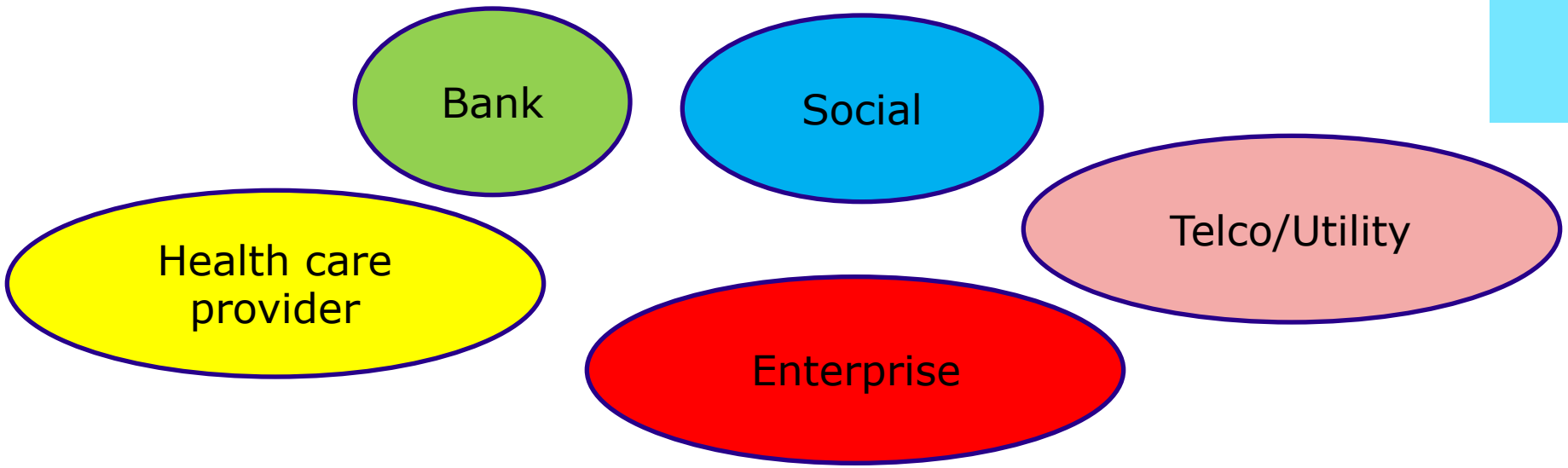
- Islands of Identity
- Continuous authentication
  - Usability & security
  - What's available today
  - Demo: Continuous Auth in action!
- The road ahead

RSA

Islands of Identity

- Building a composite of each user:
  - Our identity attributes spread across solutions we use everyday
  - WHERE should a service provider get **verified** info about a user?
  - How reliable are these attribute providers?
  - How do the attribute providers share/exchange user info?
  - Does the user **want** to share their info with the service providers?





RSA

74%

of security professionals can't tell the difference between a customer or criminal - Can You?

RSA

Islands of Identity are Complicating things

Cloud/ SaaS

Mobile

Web

On-premise

MANAGED WITH

- Multiple Products
- Different personnel
- Different policies
- Different infrastructure

CAN LEAD TO

- Rogue Access
- Shadow IT
- Lack of visibility
- Vulnerability

RSA

What is **Continuous authentication**?

What: Ongoing validation of user identity & access privileges

Why: Reduce repeated requests for users to enter credentials

How: Monitoring passive behavioral, temporal & biometric factors

Key capability: Avoid / limit direct engagement with the user

End result: Increased usability & security

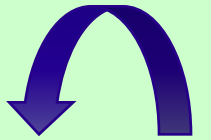
RSA

How is this different from Authentication?

Typical Authentication flow

- User tries to access a resource
- Site/resource challenges the user
- User enters credentials, Accesses resource
- To remove session: Time out occurs or user logs out

Continuous Auth flow



- User tries to access a resource
- Site/resource challenges the user
- User only asked for credentials if necessary
- Session removed if: Times out, logs out Or user activity dictates

RSA

Continuous Identity Assurance

RSA

Why continuous auth matters?

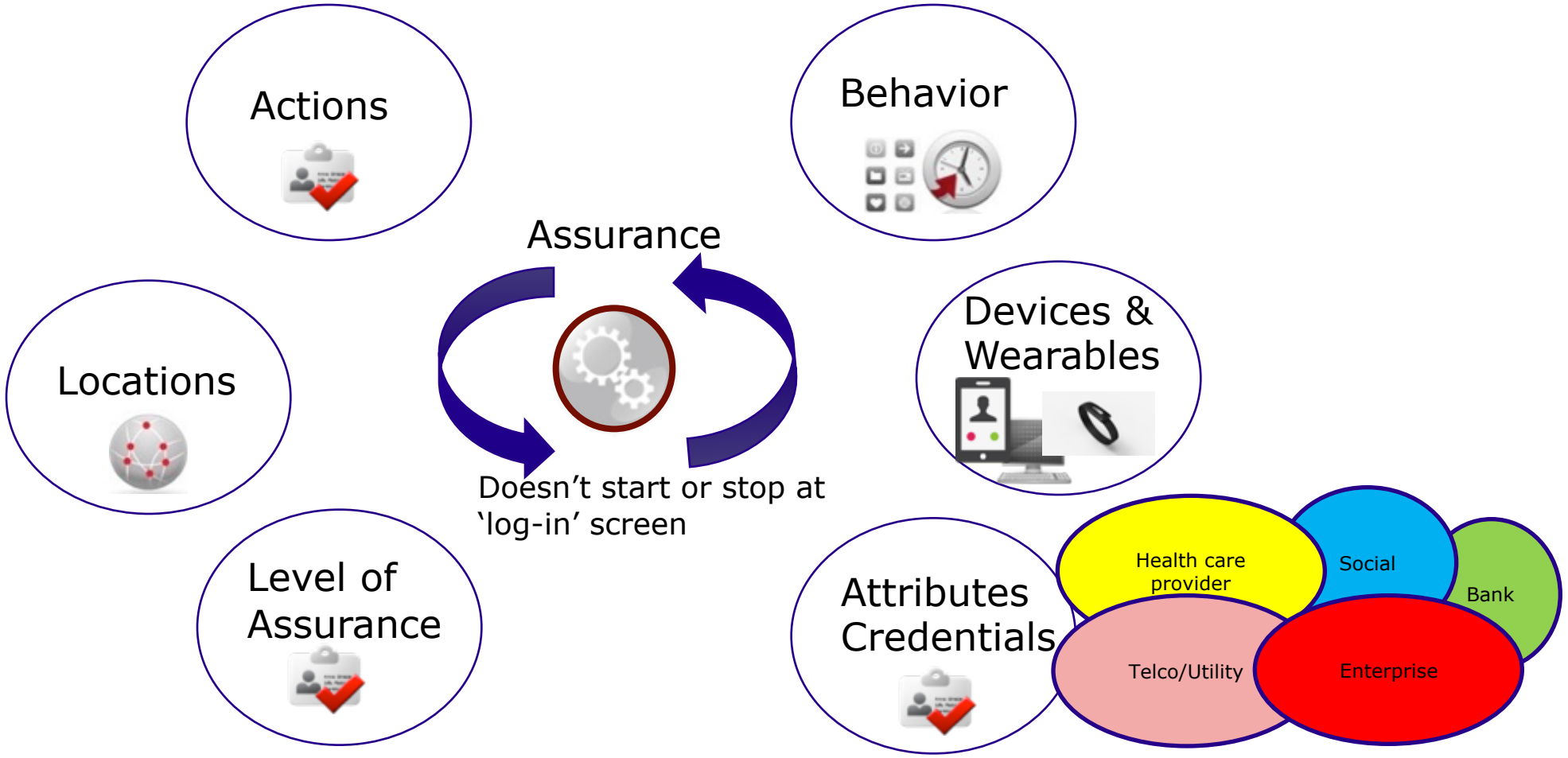
- Convenient, Frictionless
- Secure multi-factor: Who you are, What you have, Where you are
- Uses Implicit vicinity: Presence & proximity
- Various use cases:
  - Applicable to any App, Service or Resource
  - Can help Lock/Unlock devices
  - Physical Access

No, it's not a typo, we left out "what you know"…

RSA

It’s all about context!

- Contextual Authentication: Verify a user’s identity, continuously

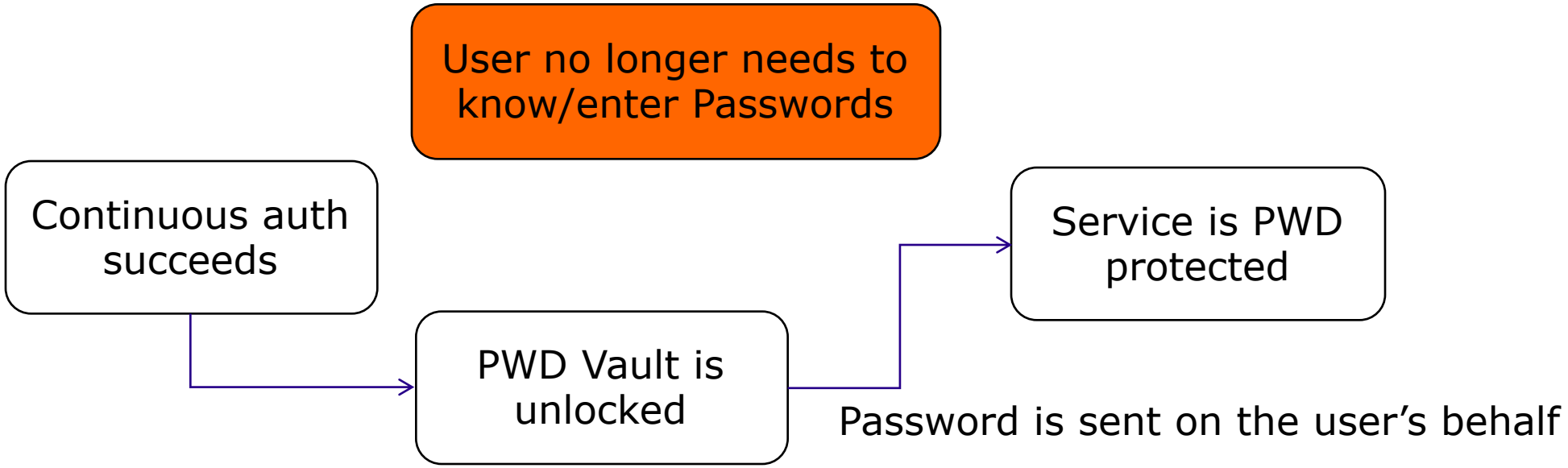


RSA

Improves Usability

- Reduced user friction /gestures
  - Silent authentication by continuously monitoring and capturing contextual data

- Coupled with Password vaulting solutions, provides better usability



RSA

Improves Security

- Reduce the threat vectors
  - By not exposing credentials as frequently as it is today
- Threats addressed
  - Leave your device unattended
  - [high value data, public areas, etc.]
- Higher assurance
  - By leveraging and continuously monitoring contextual data, and layering it on the top of user credentials or authenticated sessions
  - Coupled with Password vaulting solutions, provides higher assurance about user identity without compromising usability

What's out there

Current solutions for continuous auth

RSA

Sample implementations

- Google: Smart-Lock, Private Trust API
- Apple: Apple Watch for OS X unlock
- Microsoft: Windows Hello, Windows CDF
- Other 3rd party vendors
  - Behaviosec, EyeVerify, MacID, Knock to Unlock, etc.

Demo!

Continuous auth in action

RSA

What you'll see

Sneak peak at RSA proof of concept apps

Continuous proximity detection to Unlock/lock:

- OS X laptop, mobile device, Apple Watch & Nymi (IoT) wristband

Capabilities coming to a SecurID Access near you, very soon

RSA

The road ahead

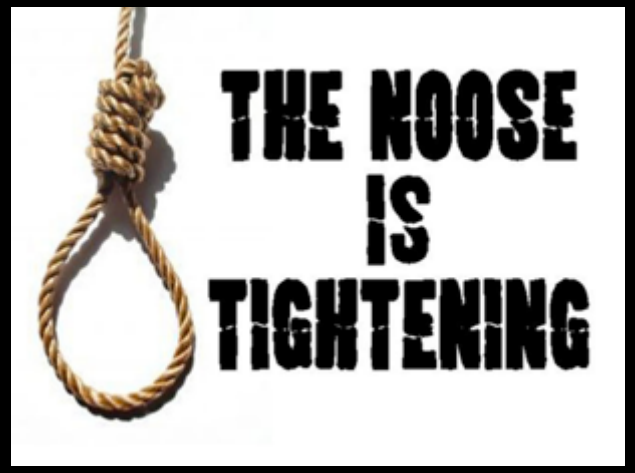
Work ahead for continuous auth

RSA

Challenges

- Not addressing enrollment
- Not a replacement for lost/stolen/backup
- Requires radios: Battery life, connectivity challenges
- BLE-based ‘distance’ is still not scientific

- If implemented incorrectly, actually creates a worse threat vector!
  - Leverage biometrics/behavioral-metrics when possible
  - Don’t depend on one 1 source of contextual data e.g. just your phone
  - Don’t depended on weak contextual data e.g. Wi-Fi and geolocation



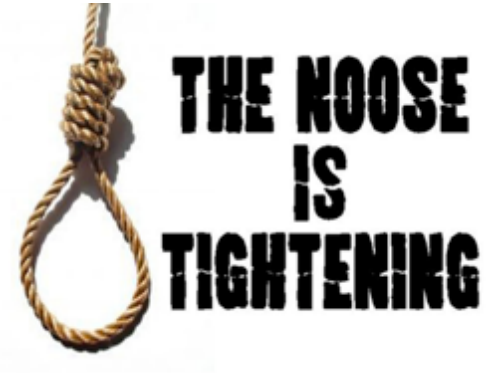
Does it kill passwords?

Can we say goodbye to Passw0rd!

RSA

Conclusion

- **What Continuous does:**
  - Reduces password friction and risks of compromise
    - Less frequent use of password by users
    - Password-less experience / invisible password when integrated with password vaults
  - Provides continuous assurance about user identity



- **What it doesn't do *yet*:**
  - Won't fully replace use of passwords in the short term

- **What fuels its success:**
  - Services and apps supporting open Auth standards (OICD, SAML)
  - Increased contextual data helps Continuous Auth, and the more likely it is to eventually…**Kill Passwords**

RSA